# *SE6 Secure Digital Systems*

**Organizer: David Money Harris,** Harvey Mudd College, Claremont, CA
**Chair: Norman Rohrer,** IBM, Essex Junction, VT

Digital security has become an essential feature in many modern systems. In 2005 and 2006, nearly one third of the residents of the United States have been informed that their personal or financial data may have been compromised by data breaches, such as the stolen Department of Veterans Affairs computer containing records on 26.5 million personnel. We depend on secure systems for electronic commerce and for the new digital economy. Music and software piracy siphons off tens of billions of dollars a year of revenues from copyright holders, yet poorly designed digital rights management angers consumers and even exposes computers to viruses. Individuals require secure communications for privacy, which is increasingly challenged as major governments monitor their own citizens.

Fortunately, algorithms for secure communication are widely known. They are generally classified as private key or public key cryptosystems. Public key systems are computationally expensive, but allow communication without first sharing a secret key between the parties. Private key systems are better suited to encrypting large amounts of data. Hence, public-key systems are generally used to encrypt short messages, sign documents, or exchange secret keys used to encrypt longer messages. Recent advances in hardware design are dramatically improving the cost, speed, and power of cryptographic hardware. Given a long enough key, these systems generally cannot be broken by brute force.

Digital systems are vulnerable to side-channel attacks that deduce information by monitoring side-effects of the encryption process. For example, delay, power consumption, or photon emissions give clues sufficient to crack many cryptosystems. Defending against these threats requires attention at many levels, including the development process, the circuit design, and the physical design.

This session will introduce the design community to public and private key algorithms with hardware implementations. Side-channel attacks will be described and demonstrated along with methods for defending against such attacks

 

**Algorithms and Hardware Design for Private Key Cryptography**

**Ingrid Verbauwhede,** K.U. Leuven, Belgium

Security is only as strong as the weakest link in the system. Mathematically very strong algorithms have been and are being developed. However, if the key leaks from the integrated circuit, this will be the weakest link. Private key algorithms, also called symmetric key algorithms, are developed with computational efficiency in mind. Examples are the recent AES algorithm and the older DES and triple-DES algorithms. Implementations are needed that can be integrated into ultra low power applications, such as RF-ID tags or extremely high throughput applications such as Gigabit IP routers. At the same time, the area and power cost should be as small as possible as the customer is not (yet) prepared to pay extra for security. In this presentation, the typical arithmetic operations, the architectures and the circuits will be presented to implement efficient, side-channel attack resistant secret key algorithms.

**Algorithms and Hardware Design for Public Key Cryptography**

**Cetin Kaya Koc**, Oregon State University & Istanbul Commerce University

Public-key cryptographic algorithms (notably RSA, Diffie-Hellman key exhcange, the Digital Signature Algorithm, and Elliptic Curve Cryptography) are based on simple mathematical structures such as finite rings and fields, and their efficient implementation in hardware requires intimate knowledge of the representation and operations with the elements of these rings and fields. A particular challenge is that these numbers are quite large, usually hundreds to thousands of bits. I will give a brief mathematical introduction to the arithmetic of rings and fields, and then introduce several hardware implementations of RSA, Diffie-Hellman and Elliptic Curve Cryptography. The field of hardware realization of public-key cryptography is still a young field, requiring advanced algorithms and design techniques in order to satisfy the requirements of the current mobile computing and communication devices as well as large systems such as IPSec routers and SSL servers.

**Side-Channel Attacks**

**Pankaj Rohatgi**, IBM T. J. Watson Research Center, Yorktown Heights, New York

Traditional cryptanalysis views a cryptographic implementation as a black boxe and assumes that the only information available to an attacker comes from the inputs and outputs of the black box. Under this assumption, most implementations that use well known cryptographic algorithms are secure provided that sufficiently large key sizes are used. However, in practice, this black box assumption does not hold and an attacker can extract valuable information about the internal operations within an implementation using side-channels such as operation timing, instantaneous power consumption, EM radiation, optical and acoustic emanations, error codes, etc. In fact, most cryptographic implementations can be easily broken using side-channel information unless measures are explicitly taken to eliminate or mitigate this information leakage. This talk will give examples and demos to illustrate the kinds of information that leaks via timing, power and EM side-channels and will explain how such information can be used to extract secret keys from devices performing cryptographic operations.

**Developing a Secure ASIC**

**Chris Curren**, EmbedICs, El Segundo, CA

The development of a secure ASIC is a process that is continually evolving. Developers continue to refine their countermeasures and leverage improvements in microelectronic technology, and attackers readily share information and learn from prior exploits. The architecture and implementation of a high volume, widely available secure ASIC that protects valuable content must use the most advanced security principles and technologies in an effort to stay ahead of adversaries while balancing the needs for manufacturability, maintainability and cost. This paper describes methods and mechanisms used when developing a secure ASIC to be resistant to a wide variety of practical and theoretical threats including social engineering, physical tampering, circuit extraction through reverse engineering, microcode extraction, bus monitoring, unexpected state transitions, circuit modification, unauthorized use, stack overflow, fault induction attacks, side-channel attacks, repeated protocol violations and the use of malicious code. A description of the threats is presented and viable countermeasures to obviate the threats are discussed.